Kentucky.gov

Commonwealth
Office of Technology

From: Ritchey, Gail (COT)
Sent: Wednesday, October 15, 2008 4:27 PM
To: COT Constitutional CIO Security Contacts; COT Cabinet CIO Security Contacts; CTC Members
Cc: COT Exchange Administrators; COT Security Alert Contacts; COT Security Contact COT-Support; COT Security Contact Pass; COT Security Contact Self-Support; COT Technical Contacts; SecurityContacts Group
Subject: COT Security Notification - Security Bulletins for October

COT Security Notification

Microsoft has just released the Security Bulletins for October which includes **four critical** bulletins, **six important** bulletins and **one moderate** bulletin. Various vulnerabilities are addressed in the bulletins. Details of the vulnerabilities and their impact are provided in the links listed.

MS08-056 Moderate: Vulnerability in Microsoft Office Could Allow Information Disclosure (957699)
http://www.microsoft.com/technet/security/bulletin/MS08-056.mspx

MS08-057 Critical: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (956416)
http://www.microsoft.com/technet/security/bulletin/MS08-057.mspx

MS08-058 Critical: Cumulative Security Update for Internet Explorer (956390)
http://www.microsoft.com/technet/security/bulletin/MS08-058.mspx

MS08-059 Critical: Vulnerability in Host Integration Server RPC Service Could Allow Remote Code Execution (956695)
http://www.microsoft.com/technet/security/bulletin/MS08-059.mspx

MS08-060 Critical: Vulnerability in Active Directory Could Allow Remote Code Execution (957280)
http://www.microsoft.com/technet/security/bulletin/MS08-060.mspx

MS08-061 Important: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (954211)
http://www.microsoft.com/technet/security/bulletin/MS08-061.mspx

MS08-062 Important: Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution (953155)
http://www.microsoft.com/technet/security/bulletin/MS08-062.mspx

MS08-063 Important: Vulnerability in SMB Could Allow Remote Code Execution (957095)
http://www.microsoft.com/technet/security/bulletin/MS08-063.mspx

MS08-064 Important: Vulnerability in Virtual Address Descriptor Manipulation Could Allow Elevation of Privilege (956841)
http://www.microsoft.com/technet/security/bulletin/MS08-064.mspx

MS08-065 Important: Vulnerability in Message Queuing Could Allow Remote Code Execution (951071)
http://www.microsoft.com/technet/security/bulletin/MS08-065.mspx

MS08-066 Important: Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege (956803)
http://www.microsoft.com/technet/security/bulletin/MS08-066.mspx

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Confidentiality Statement - This communication contains information which is confidential. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any form of distribution, copying, forwarding or use of this communication or the information therein is strictly prohibited and may be unlawful. If you have received this communication in error, please return it to the sender and send a copy or notify: securitynotice@ky.gov and then delete the communication and destroy any copies.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601

COTSecurityServicesISS@ky.gov
http://technology.ky.gov/security/